CLAIMS

We claim:

1. A method of transferring personal information of a plurality of users from a first computer in which said personal information is identifiable with particular users to a second computer in which said personal information is de-identified, said method comprising the steps:

transferring de-identified personal information of said users from said first computer to said second computer;

transferring identifiable personal information from said first computer to a third computer;

generating on said third computer an anonymous ID for each user which anonymously identifies the user;

transferring said anonymous IDs from said third computer to said second computer;

correlating said anonymous IDs with said de-identified personal information on said second computer; and

storing in a database accessible to said second computer said de-identified personal information of said users indexed by anonymous ID.

2. The method according to claim 1 wherein said anonymous IDs transferred from said third computer to said second computer are encrypted under an encryption key maintained by said third computer.

3. The method according to claim 2 wherein said de-identified personal information of said users is indexed by encrypted anonymous ID.

4. The method according to claim 1 wherein said anonymous IDs are transferred from said third computer to said second computer via a virtual private network within the public Internet.

5. The method according to claim 1 including the additional step of transferring said indexed de-identified personal information from said database to a data warehouse.

6. The method according to claim 5 including the additional step of transferring said indexed de-identified personal information from said data warehouse to a World-Wide-Web (WWW) site.

7. The method according to claim 1 wherein said first computer is operated by a health plan and wherein said users are members of said health plan.

8. The method according to claim 1 wherein said second computer is operated by an operator of a WWW site.

9. The method according to claim 1 wherein said third computer is operated by a registration authority.

10. The method according to claim 1 wherein said de-identified personal information is medical claims data and wherein said identifiable personal information is eligibility data of said users.

11. The method according to claim 1 wherein said de-identified personal information of said users is financial information of said users.

12. The method according to claim 1 wherein said de-identified personal information of said users is employee benefits information of said users.

13. The method according to claim 1 wherein:

said de-identified personal information transferred from said first computer to said second computer is indexed by surrogate IDs assigned to each user by said first computer, said surrogate IDs being encrypted using an encryption key maintained by said first computer;

said identifiable personal information transferred from said first computer to said third computer is indexed by unencrypted surrogate IDs;

said encryption key is transferred to said third computer from said first computer;

said third computer encrypts said surrogate IDs using said encryption key and transfers said encrypted surrogate IDs to said second computer with said anonymous IDs; and

said second computer uses said encrypted surrogate IDs transferred from said third computer to correlate said anonymous IDs with said de-identified personal information received from said first computer.

14. A method of receiving personal information of a plurality of users, said method comprising the steps:

receiving at a second computer de-identified personal information of said users transferred from a first computer;

receiving at said second computer anonymous IDs for each of said users which anonymously identify each user transferred from a third computer;

correlating on said second computer said anonymous IDs with said de-identified personal information; and

storing in a database accessible to said second computer said de-identified personal information of said users indexed by anonymous ID.

15. The method according to claim 14 wherein said anonymous IDs received by said second computer are encrypted under an encryption key maintained by said third computer.

16. The method according to claim 15 wherein said de-identified personal information of said users is indexed in said database by encrypted anonymous ID.

17. The method according to claim 14 wherein said anonymous IDs are transferred from said third computer to said second computer via a virtual private network within the public Internet.

18. The method according to claim 14 including the additional step of transferring said indexed de-identified personal information from said database to a data warehouse.

19. The method according to claim 14 wherein said second computer is operated by an operator of a WWW site.

20. The method according to claim 14 wherein said third computer is operated by a registration authority.

21. The method according to claim 14 wherein said de-identified personal information is medical claims data and wherein said identifiable personal information is eligibility data of said users.

22. The method according to claim 14 wherein said de-identified personal information of said users is financial information of said users.

23. The method according to claim 14 wherein said de-identified personal information of said users is employee benefits information of said users.

24. The method according to claim 14 wherein:

said de-identified personal information received by said second computer is indexed by surrogate IDs assigned to each user by said first computer, said surrogate IDs being encrypted using an encryption key maintained by said first computer;

said identifiable personal information transferred from said first computer to said third computer is indexed by unencrypted surrogate IDs;

said encryption key is transferred to said third computer from said first computer;

said third computer encrypts said surrogate IDs using said encryption key and transfers said encrypted surrogate IDs to said second computer with said anonymous IDs; and

said second computer uses said encrypted surrogate IDs transferred from said third computer to correlate said anonymous IDs with said de-identified personal information received from said first computer.

25. A method of registering an anonymous user of a World-Wide-Web (WWW) site, said user requiring a valid Web ID and password to log on to said WWW site, said method comprising the steps:

verifying the identity of said anonymous user on a first server;

if the identity of said anonymous user is verified, creating and storing said password on a second server;

if a password is created, creating and storing said Web ID on a third server;

wherein the only party that has access to the identity, Web ID and password of the anonymous user is the user.

26. The method according to claim 25 wherein on log-ins to the WWW site by said user said password is verified by said second server and said Web ID is separately verified by said third server.

27. The method according to claim 25 wherein said first server and said second server are the same server.

28. The method according to claim 25 wherein said first server and said second server are different servers.

29. A method of registering an anonymous user of a World-Wide-Web (WWW) site, said user requiring a valid Web ID and digital certificate to log on to said WWW site, said method comprising the steps:

verifying the identity of said anonymous user on a first server;

if the identity of said anonymous user is verified, creating said digital certificate on a second server and storing said digital certificate on a computer which will be used by said user to access said WWW site;

wherein the only party that has access to the identity, Web ID and digital certificate of the user is the user.

30. The method according to claim 29 wherein on log-ins to the WWW site by said user said digital certificate is verified by said second server and said Web ID in separately verified by a third server.

31. The method according to claim 29 wherein said first server and said second server are the same server.

32. The method according to claim 29 wherein said first server and said second server are the different servers.

33. A method of processing a computer-generated communication, said method comprising the steps:

generating a transaction token on a second computer and uploading said transaction token to a first computer over a first communications network;

linking, over said first communications network, said first computer to a third computer that will process said communication; and

transferring said communication from said second computer to said third computer, said communication being transferred to said third computer over a second communications network;

wherein said first computer presents said transaction token to said third computer over said first communications network for validation and wherein said third computer processes said communication only if said transaction token is valid.

34. The method according to claim 33 wherein said transaction token is valid for a finite time period and wherein said token must be presented to said third computer within said finite time period if said token is to be validated.

35. The method according to claim 33 wherein said first communications network is the public Internet and wherein said second communications network is a virtual private network within the public Internet.

36. The method according to claim 33 wherein said first computer is a personal computer and wherein said second and third computer are server computers.

37. The method according to claim 33 wherein said second computer transfers a portion of said transaction token to said third computer and wherein said third computer uses said transaction token portion in validating said transaction token.

38. The method according to claim 37 wherein said transaction token portion is a transaction token number.

39. The method according to claim 37 wherein said communication is a request.

40. The method according to claim 37 wherein said communication is a response.

41. A system for transferring personal information of a plurality of users from a first computer in which said personal information is identifiable with particular users to a second computer in which said personal information is de-identified, said system comprising:

a first computer containing personal information of said users;

a second computer for receiving de-identified personal information of said users transferred from said first computer;

a third computer for receiving identifiable personal information transferred from said first computer;

said third computer being configured to generate an anonymous ID for each user which anonymously identify the user and transfer said anonymous IDs to said second computer;

said second computer being configured to correlate said anonymous IDs with said de-identified personal information and store said de-identified information in a database accessible to said second computer indexed by anonymous ID.

42. The system according to claim 41 wherein said third computer is further configured to encrypt said anonymous IDs under an encryption key maintained by said third computer prior to transferring said anonymous IDs to said first computer.

43. The system according to claim 42 wherein said de-identified personal information of said users is indexed in said database by encrypted anonymous ID.

44. The system according to claim 41 wherein said anonymous IDs are transferred from said third computer to said second computer via a virtual private network within the public Internet.

45. The system according to claim 41 wherein said second computer is further configured to transfer said indexed de-identified personal information from said database to a data warehouse.

46. The system according to claim 41 wherein said indexed de-identified personal information is transferred from said data warehouse to a World-Wide-Web (WWW) site.

47. The system according to claim 41 wherein said first computer is operated by a health plan and wherein said users are members of said health plan.

48. The system according to claim 41 wherein said second computer is operated by an operator of a WWW site.

49. The system according to claim 41 wherein said third computer is operated by a registration authority.

50. The system according to claim 41 wherein said de-identified personal information of said users is medical claims data and wherein said identifiable personal information is eligibility data.

51. The system according to claim 41 wherein said de-identified personal information of said users is financial information of said users.

52. The system according to claim 41 wherein said de-identified personal information of said users is employee benefits information of said users.

53. The system according to claim 41 wherein:

said de-identified personal information transferred from said first computer to said second computer is indexed by surrogate IDs assigned to each user by said first computer, said surrogate IDs being encrypted using an encryption key maintained by said first computer;

said identifiable personal information transferred from said first computer to said third computer is indexed by unencrypted surrogate IDs;

said first computer transfers said encryption key to said third computer;

said third computer encrypts said surrogate IDs using said encryption key and transfers said encrypted surrogate IDs to said second computer with said anonymous IDs; and

said second computer uses said encrypted surrogate IDs transferred from said third computer to correlate said anonymous IDs with said de-identified personal information received from said first computer.

54. A system for receiving personal information of a plurality of users comprising:

a computer, said computer being configured to (1) receive de-identified personal information of said users transferred from a second computer, (2) receive anonymous IDs for each of said users transferred from a third computer, (3) correlate said anonymous IDs with

said de-identified personal information, and (4) store in an accessible database said de-identified personal information of said users indexed by anonymous ID.

55. The system according to claim 54 wherein said anonymous IDs received from said third computer are encrypted under an encryption key maintained by said third computer.

56. The system according to claim 55 wherein said de-identified personal information of said users is indexed by encrypted anonymous ID.

57. The system according to claim 54 wherein said anonymous IDs are transferred from said third computer to said computer via a virtual private network within the public Internet.

58. The system according to claim 54 wherein said computer transfers said indexed de-identified personal information to a data warehouse.

59. The system according to claim 54 wherein said computer is operated by an operator of a WWW site.

60. The system according to claim 54 wherein said third computer is operated by a registration authority.

61. The system according to claim 54 wherein said de-identified personal information is medical claims data and wherein said identifiable personal information is eligibility data.

62. The system according to claim 54 wherein said de-identified personal information of said users is financial information of said users.

63. The system according to claim 54 wherein said de-identified personal information of said users is employee benefits information of said users.

64. The system according to claim 54 wherein:

said de-identified personal information received by said computer is indexed by surrogate IDs assigned to each user by said second computer, said surrogate IDs being encrypted using an encryption key maintained by said second computer;

said identifiable personal information on said third computer is indexed by unencrypted surrogate IDs;

said encryption key is transferred to said third computer from said second computer;

said third computer encrypts said surrogate IDs using said encryption key and transfers said encrypted surrogate IDs to said computer with said anonymous IDs; and

said computer uses said encrypted surrogate IDs transferred from said third computer to correlate said anonymous IDs with said de-identified personal information received from said computer.

65. A system for registering an anonymous user of a World-Wide-Web (WWW) site, said user requiring a valid Web ID and password to log on to said WWW site, said system comprising:

a first server for verifying the identity of said anonymous user;

a second server for creating and storing said password if the identity of said anonymous user is verified by said first server, and

a third server for creating and storing said Web ID if said password is created by said second server;

wherein the only party that has access to the identity, web ID and password of the anonymous user is the user.

66. The system according to claim 65 wherein on log-ins to the WWW site by said user said password is verified by said second server and said Web ID is separately verified by said third server.

67. The system according to claim 65 wherein said first server and said second server are the same server.

68. The system according to claim 65 wherein said first server and said second server are different servers.

69. A system for registering an anonymous user of a World-Wide-Web (WWW) site, said user requiring a valid Web ID and digital certificate to log on to said WWW site, said method comprising the steps:

a first server for verifying the identity of said anonymous user;

a second server for creating said digital certificate and storing said digital certificate on a computer which will be used by said user to access said WWW site password if the identity of said anonymous user is verified by said first server;

wherein the only party that has access to the identity, Web ID and digital certificate of the anonymous user is the user.

70. The system according to claim 69 wherein on log-ins to the WWW site by said user said digital certificate is verified by said second server and said Web ID in separately verified by a third server.

71. A system for processing a computer-generated communication comprising:

a first computer, a second computer and third computer;

said second computer being configured to generate a transaction token, upload said transaction token to said first computer over a first communications network, and link said first computer to said third computer over said first communications network;

said second computer being further configured to transfer said communication to said third computer over a second communications network,

said first computer being configured to present said transaction token to said third computer over said first communications network for validation;

said third computer being configured to validate said transaction token and process said communication only if said transaction token is valid.

72. The system according to claim 71 wherein said transaction token is valid for a finite time period and wherein said token must be presented to said third computer within said finite time period if said token is to be validated.

73. The system according to claim 71 wherein said first communications network is the public Internet and wherein said second communications network is a virtual private network within the public Internet.

74. The system according to claim 71 wherein said first computer is a personal computer and wherein said second and third computer are server computers.

75. The system according to claim 71 wherein said second computer transfers a portion of said transaction token to said third computer with said communication and wherein said third computer uses said transaction token portion in validating said transaction token.

76. The system according to claim 71 wherein said transaction token portion is a token transaction number.

77. The system according to claim 71 wherein said communication is a request.

78. The system according to claim 71 wherein said communication is a response.

79. A system for processing a computer-generated communication comprising:

a computer, said second computer being configured to (1) generate a transaction token, (2) upload said transaction token to a first computer over a first communications network, (3) link said first computer to a third computer over said first communications network, and (4) transfer said communication to said third computer over a second communications network;

wherein said first computer presents said transaction token to said third computer over said first communications network for validation; and

wherein said third computer validates said transaction token and processes said communication only if said transaction token is valid.